INTRUSION DETECTION SYSTEM And Its Variations

[1]Shivam Singh, [2]Omkar Shendre, [3]Nilesh Gujar, [4]Himanshu Agarwal, [5]Ratan Singh
Student , [2]Student, [3]Student, [4]Student, [5]Professor Cloud Technology and Information Security
Ajeenkya Dy Patil Univrsity, Pune , Maharashtra

ABSTRACT **:** Intrusion Detection System (IDS) is a software application that monitors network or system activity and detects any malicious activity. The tremendous growth and use of the Internet raises concerns about how to protect and transmit digital information in a secure way. Currently, hackers use various types of attacks to obtain valuable information. Many intrusion detection methods, techniques and algorithms help detect these attacks. This main goal of this article is to provide a complete study on the definition of intrusion detection, history, types of intrusion detection, types of attacks, various tools.

KEYWORDS : Intrusion detection, Functionality, IDS attacks and Types,Tools.

1. INTRODUCTION : An intrusion detection system is an application or software used to monitor the network and protect it from the intruder. With the rapid progress in Internet-based technology, new areas of application for the computer network have emerged. In some cases, the fields of business, finance, industry, safety and health, LAN and WAN applications have progressed. All these areas of application made the network an attractive target for abuse and a great vulnerability for the community. Malicious users or hackers use the internal systems of the organization to collect information and cause vulnerabilities such as software errors, expiration in administration, leaving the systems to the default settings. As the Internet emerges in society, new things like viruses and worms are imported. The wrong then, users use different techniques such as decrypting the password, unencrypted text detection is used to cause vulnerabilities in the system. Therefore, security is needed for users to secure their system from intruders. The firewall technique is one of the most popular protection techniques and is used to protect the private network from the public network. IDSs are used in network-related activities, medical applications, credit card fraud, insurance agencies.

2. History : The purpose of intrusion detection is to monitor network assets to detect abnormal behavior and abuse in the network. Intrusion detection concept was introduced in the early 1980s after the evolution of the internet with surveillance and monitoring of the threat. There was a sudden increase in reputation and integration in security infrastructure. Since then, various events in IDS technology have advanced intrusion detection to the current status. James Anderson's wrote a paper for a government organization and imported an approach where audit trails contain important information that could be useful in tracking abuse and understanding of user behavior.

Then the detection and control data appeared and their importance led to great improvements in the subsystems of each operating system. IDS and Host Based Intrusion Detection System (HIDS) were first defined. In 1983, SRI International and Dorothy Denning started working on a government project that made a new effort for the development of intrusion detection systems. Around the 1990s, revenues are generated and the market for burglary detection is increased. Real secure is a burglary detection network developed by ISS. After a year, Cisco recognized the priority for network intrusion detection and the Wheel Group purchased to achieve security solutions. The government actions such as Federal Intrusion Detection Networks (FID Net) are designed within the framework of the Presidential Decision Directive 63 and also give an impetus to the IDS.

3. **INTRUSION DETECTION SYSTEM :** The purpose of intrusion detection is to monitor network resources to detect abnormal behavior and network abuse. The intrusion detection concept was introduced in the early 1980s after the evolution of the Internet with threat surveillance and monitoring. There has been a sudden increase in reputation and integration in the security infrastructure. Since then, various events in IDS technology have advanced intrusion detection to the current state. James Anderson's wrote a document for a government organization and imported an approach in which audit trails contain important information that could be useful in tracking abuse and understanding user behavior.
So survey and control data appeared and their importance led to great improvements in the subsystems of each operating system. IDS and Host Based Intrusion Detection System (HIDS) were initially defined. In 1983, SRI International and Dorothy Denning started working on a government project that made a new effort to develop intrusion detection systems. Around the 90s, revenue is generated and the market for burglary theft is increased. Real Secure is a burglary detection network developed by ISS. After a year, Cisco recognized the priority for network intrusion detection and the Wheel Group purchased to get security solutions. Government actions such as federal intrusion detection networks (FID network) are designed under the Presidential Decision Directive 63 and also give impetus to the IDS.

3.1 TYPES OF IDS: Host based IDS
Network based IDS

3.1.1HIDS

Host based IDS views the sign of intrusion in the local system. For analysis they use host system's logging and other information. Host based handler is referred as sensor. Other sources, from which a host-based sensor can obtain data, include system logs and other logs generated by operating system processes and contents of objects not reflected in standard operating system audit and logging mechanisms . Host based system trust strongly on audit trail. The information allows the intrusion detection system to spot subtle patterns of misuse that would not be visible at a higher level of abstraction . The elementary principle in IDS including Network Based Intrusion Detection System (NIDS) originated from anomaly HIDS research based on Denning's pioneering work. A host-based IDS provides much more relevant information than Network-based IDS. HIDS are used efficiently for analyzing the network attacks, for example, it can sometimes tell exactly what the attacker did, which commands he used, what files he opened, rather than just a vague accusation and there is an attempt to execute a dangerous command. It is less risky to configure.

ADVANTAGES OF HIDS

- Verifies success or failure of an attack
- Monitors System Activities
- Detects attacks that a network based IDS fail to detect
- Near real time detection and response
- Does not require additional hardware
- Lower entry cost

3.1.2 NIDS

Network-based IDS systems collect information about the network itself rather than about each separate host . NIDS audits network attacks when transferring packets over the network. Network sensors are equipped with attack signatures that determine what will constitute an attack. Most network-based systems allow advanced users to define their own signatures . The attack on the sensor is based on the signature and they are from previous attacks and the operation of the monitors will be transparent to the users, which is also significant

ADVANTAGES OF NIDS

- Lower Cost of Ownership
- Easier to deploy
- Detect network based attacks
- Retaining evidence Real Time detection and quick response.
- Detection of failed attacks\
-

3.2 IDS FUNCTIONS

Data collection :This module captures the data as an input to the IDS. The data is recorded on file and then analyzed. Collects and converts IDS based on the network of data packets and collects the host IDS data such as disk usage and system processes.
Feature Selection :In order to select the particular feature large data is available in the network and they are usually evaluated for disruption. For example, the Internet Protocol (IP) address of the source and target system, the type of protocol, the length and the size of the headers could be accepted as the key for submission .

Analysis :Data is analyzed to determine accuracy. IDS-based rules makes analysis of the data in which incoming traffic is checked against signatures or a predefined pattern . Another method is IDS based on an anomaly that studies the behavior of the system and uses mathematical models .

Action : It defines the attack and reaction of the system. The system administrator can inform all necessary data by email / alarm icons or can actively participate in the system by omitting packets so that it does not enter the system or close the ports.

4.ATTACKS

3.1. Denial-of-Service (DOS) Attacks
It tries to deny the authorized users from promoting the requested service. An advanced Distributed Denial of Service occurs in a distributed environment that the attacker sends or floods the server with numerous connection that request to knock the target system .Types of DOS attacks are

4.1.1. SYN Attack
SYN attack is also defined as Synchronization attack. Here, the attacker sends the flood of SYN request to the destination to use the resources of the server and to make the system unresponsive.

4.1.2. Ping of Death
In this the intruder sends a ping request to the targeted system which is larger than 65,536 bytes which causes the system to crash. The formal size must be 56 bytes or 84 bytes incase of considering Internet protocol header.

4.2. Eavesdropping Attacks

It is the scheme of interference in communication by the attacker. This attack can be done over by telephone l lines or through email..

4.3 Spoofing Attacks

This attacker portrays as another user to forge the data and take advantages on illegal events in the network. IP spoofing is a common example where the system communicates with a trusted user and provides access to the attacker .

4.4. Intrusion attacks or User to Root Attack (U2R)

An intruder tries to access the system or route through the network. Buffer overflow attack is a typical intrusion attack which occurs when a web service receives more data than it has been programmed to handle which leads to loss of data .

4.5. Logon Abuse Attacks

A logon abuse attack would neglect the authentication and access control mechanisms and grant a user with more advantages .

4.6 Application-Level Attacks

The attacker targets the disabilities of application layer. For example, security weakness in the web server or in faulty controls on the server side

5. TOOLS IN INTRUSION DETECTION

An intrusion detection product available today addresses a range of organizational security goals .This section discusses about the security tools.

5.1 SNORT

Snort is lightweight and open source software. Snort uses a flexible rule-based language to describe the traffic .From an IP address; it records the packet in human readable form.Through protocol analysis, content searching, and various pre-processors Snort detects thousands of worms, vulnerability exploit attempts, port scans, and other suspicious behavior .

5.2 OSSEC-HIDS

OSSEC (open source security) is free open source software. It will run on major operating system and uses a Client/Server based architecture. OSSEC has the ability to send OS logs to the server for analysis and storage. It is used in powerful log analysis engine, ISPs, universities and data centres. Authentication logs, firewalls are monitored and analysed by HIDS.

5.3 FRAGROUTE

It is termed as fragmenting router. Here, from the attacker to the fragrouter the IP packet is sent and they are then fragmented and transformed to the party.

5.4 HONEYD

Honeyd is a tool that creates virtual hosts on the network. The services are used by the host Honeyd allows a single host to request multiple addresses on a LAN for networks simulation. It is possible to knock the virtual machines or to trace route them. Any type of service on the virtual machine can be simulated according to a simple configuration file .

6. IDS IN VARIOUS DOMAINS.

An IDS is used in numerous fields and the performance in each field is described and defines how they performed.

6.1 IDS in MANET

The handle is defined as a mobile adhoc network. It is an autonomous network that is naturally composed by combinations of mobile nodes without centralized administration. SID is used in the handle. The mobile network is normally required on the battlefield for the military to obtain an adequate network . Normally, messages are divided into packages and use a hardware device such as wire and modem to transmit. But in Manet they are connected wirelessly. Warfare and qualifier are the two techniques added to the protocol in Adhoc.

A security guard identifies the inappropriate behavioral nodes by transmitting the ears when transmitting the next jump. A path qualifier then helps to find routes that do not contain those nodes. The IDs are used in Manet while transferring the packet series to the destination via the mobile network to find the intruder if any.

6.2 IDS FOR CLOUD COMPUTING

Cloud computing is illustrated as an Internet computing cloud where virtual shared servers provide software infrastructure platform devices and other resources, and provide customer service as a paid service as you use . The cloud user does not have any physical framework, instead renting from an intermediary (third party). They only pay for resource use. The burglary detection system plays an important role in the security and perseverance of an active defense system against hostile attacks against any business and IT organization . In cloud computing, applications are received on a remote server and have control over data usage. IDMEF (Entry Detection Messaging Format) is a standard used in the cloud for communication purposes

6.3 IDS in Data Mining

Data mining is the process of extracting hidden knowledge from databases. IDSs are very important in digging data. Detecting a burglary involves identifying a set of malicious actions that compromise the integrity and availability of information sources .

Detecting a burglary into data digging has two divisions, that is, misuse detection and anomaly detection. In the detection of misuse, labeled data are produced according to a prediction model. There is a discrepancy between the models in detecting the anomaly. To use the data for the first time, it must be converted to
it is subject to prominent data and data extraction models that are summarized to produce a result.

7. **CONCLUSION:** The main purpose of this paper is to provide an overview of the need for and use of intrusion detection systems. This paper provides a complete study of IDS types, life cycles, various domains, types of attacks and tools. IDS is important for security today in the corporate world and for network users. IPS defines prevention measures for security. In the life cycle the phases are developed and the stages are illustrated. However, there are still many challenges to overcome. Anomaly detection and abuse detection techniques are specifically illustrated and more techniques can be used. Further work will be carried out on the comparative analysis of
several popular data mining algorithms that are applied to IDS and improve classification based on IDS using selective feedback methods.

REFERENCES:

[1] Corinne Lawrence- "IPS – The Future of Intrusion Detection"- University of Auckland - 26th October 2004.

[2] Karthikeyan .K.R and A. Indra- "Intrusion Detection Tools and Techniques a Survey"

[3] Anita K. Jones and Robert S. Sielken –"Computer System Intrusion Detection A Survey "International Journal of Computer Theory and Engineering, Vol.2, No.6, December, 2010

[4] Vera Marinova-Boncheva-"A Short Survey of Intrusion Detection Systems"-. Bulgarian academy of sciences.

[5] Shankar Sharan Tripathi, Sonu Agrawal- "A Survey on Enhanced Intrusion Detection System in Mobile Ad hoc Network"- International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 7, September 2012.

[6] Ms. Parag K. Shelke, Ms. Sneha Sontakke, Dr. A. D. Gawande – "Intrusion Detection System for Cloud Computing". International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012 ISSN 2277-8616 67 IJSTR©2012.

[7] Paul Dokas, Levent Ertoz, Vipin Kumar, Aleksandar Lazarevic, Jaideep Srivastava, Pang-Ning Tan"Data Mining for Network Intrusion Detection".

[8] Aleksandar Lazarević,Jaideep Srivastava, Vipin Kumar-"Data Mining for intrusion detection"Tutorial on the
Pacific-Asia Conference on Knowledge Discovery in Databases 2003. [